FIG.1a.

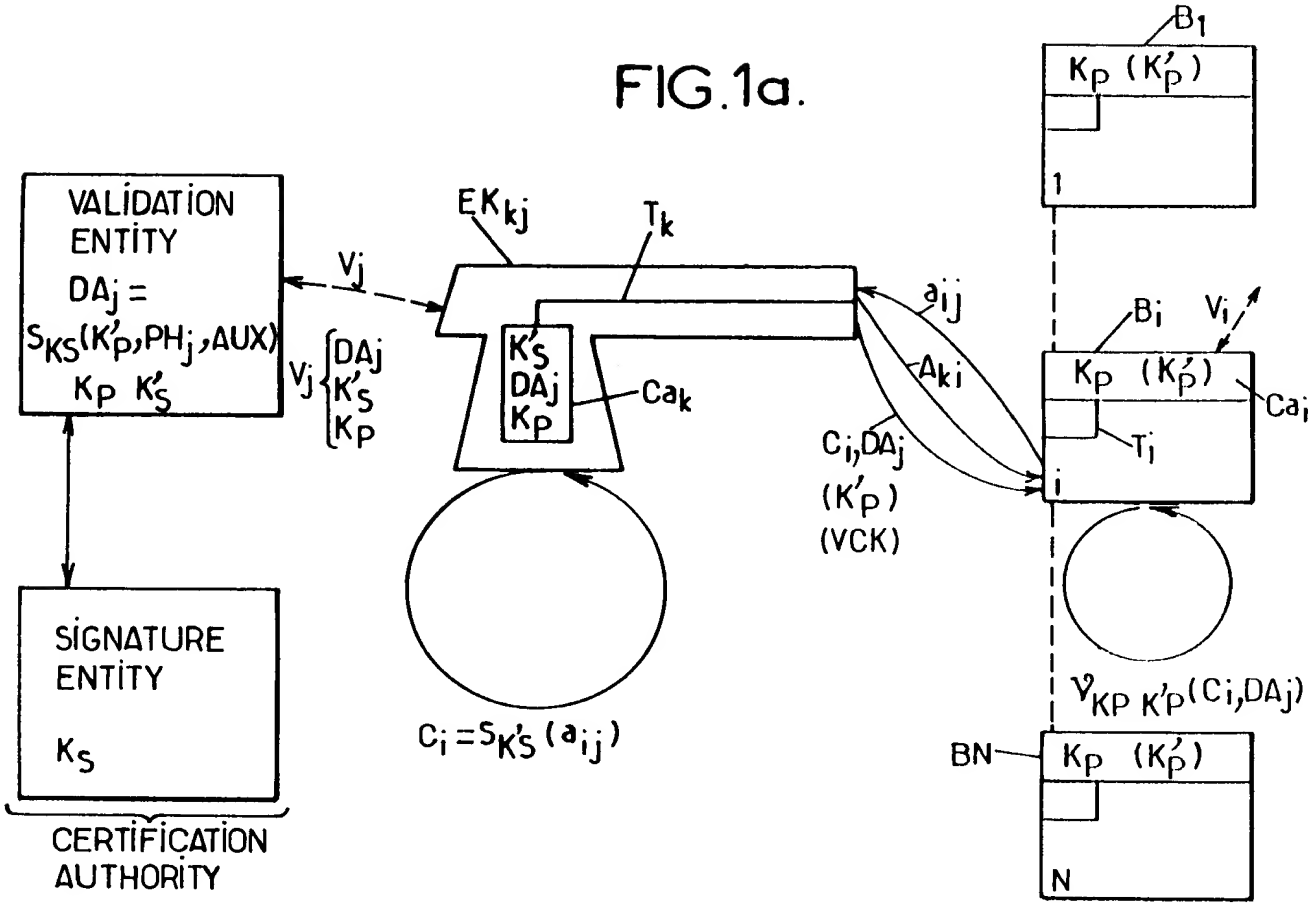

VALIDATION ENTITY
DAj = SKS(K'P,PHj,AUX)
KP K'S
SIGNATURE ENTITY
KS
CERTIFICATION AUTHORITY
Vj
Vj {DAj K'S KP
EKkj
Tk
K'S DAj KP
Cak
Ci=SK'S(aij)
aij
Aki
Ci,DAj (K'P) (VCK)
B1
KP (K'P)
1
Bi
Vi
Cai
Ti
i
BN
N
V KP K'P(Ci,DAj)

FIG.1b.

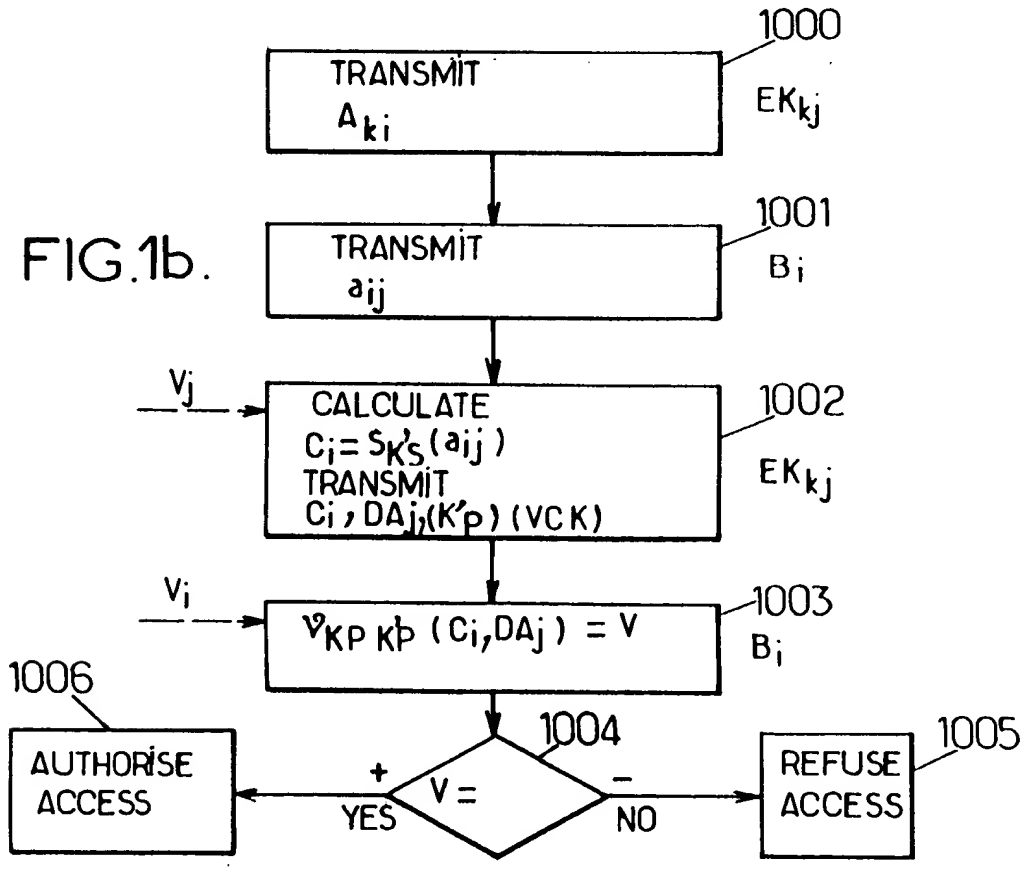

TRANSMIT Aki
1000
EKkj
TRANSMIT aij
1001
Bi
Vj
CALCULATE Ci=SK'S(aij) TRANSMIT Ci, DAj,(K'P) (VCK)
1002
EKkj
Vi
V KP K'P (Ci,DAj) = V
1003
Bi
1004
V=
+
YES
−
NO
1006
AUTHORISE ACCESS
1005
REFUSE ACCESS

FIG.1c.

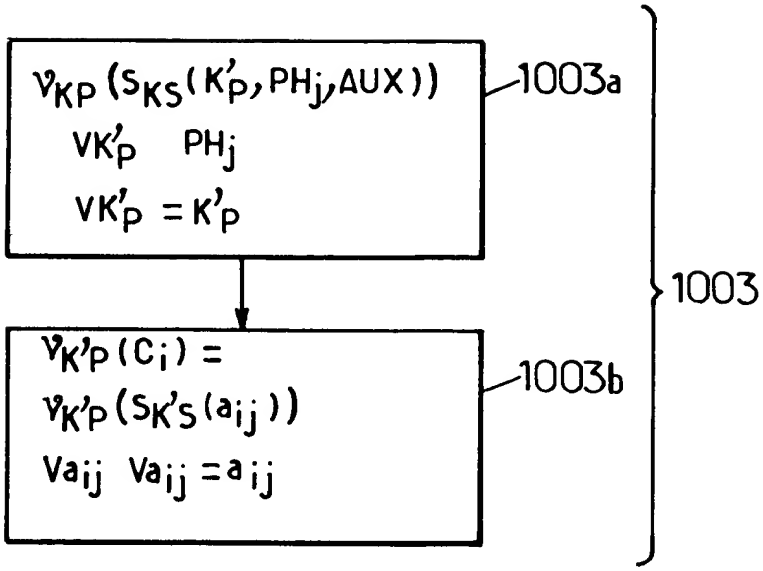


FIG.1d.

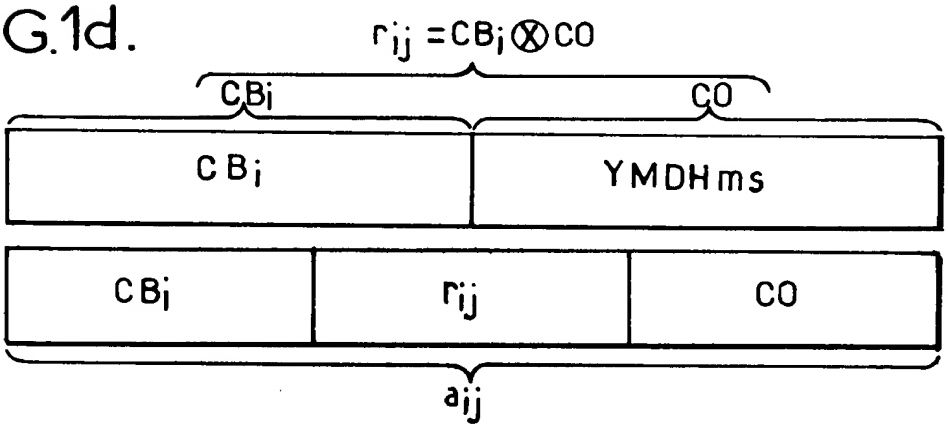
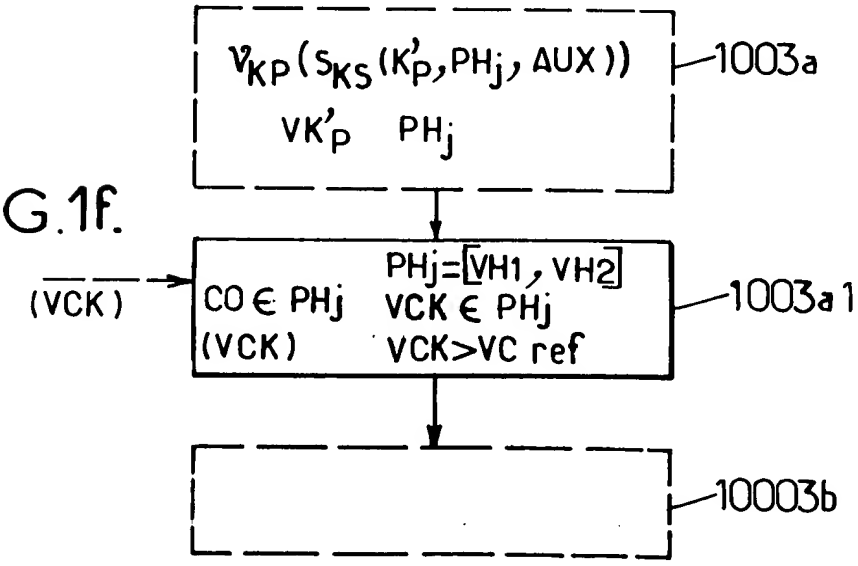


FIG.1f.



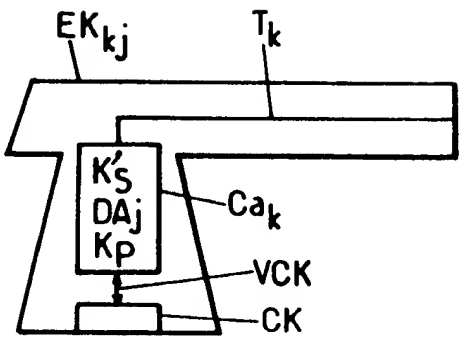

EK_kj
T_k
K'_S
DAj
K_P
Ca_k
VCK
CK

FIG.1e.

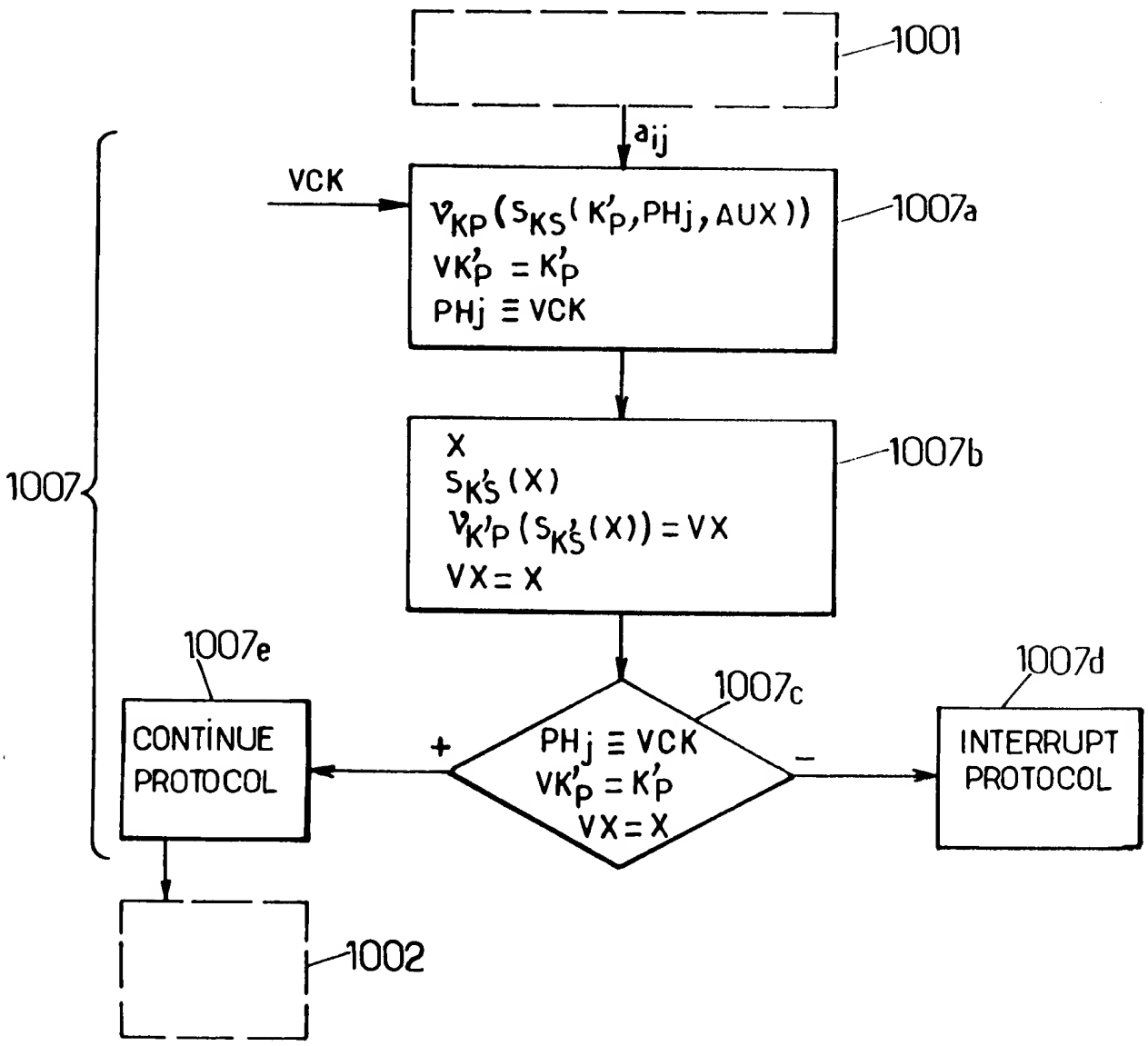

1001
a_ij
VCK
V_KP(S_KS(K'_P, PHj, AUX))
VK'_P = K'_P
PHj ≡ VCK
1007a
X
S_K'S(X)
V_K'P(S_K'S(X)) = VX
VX = X
1007b
1007
1007e
CONTINUE PROTOCOL
1007c
PHj ≡ VCK
VK'_P = K'_P
VX = X
+
−
1007d
INTERRUPT PROTOCOL
1002

FIG. 1g.

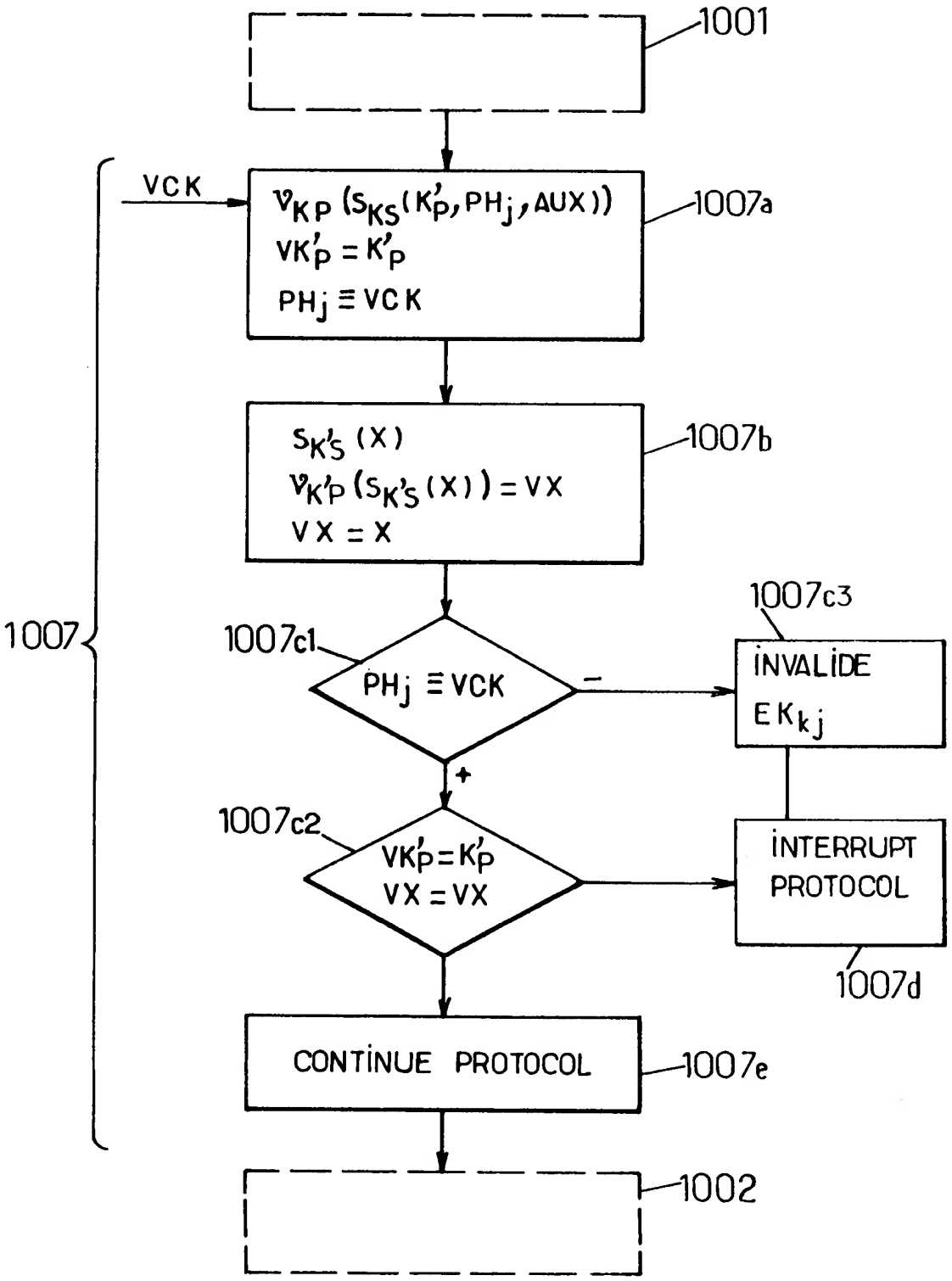

1001
VCK
$v_{KP}(s_{KS}(K'_P, PH_j, AUX))$
$VK'_P = K'_P$
$PH_j \equiv VCK$
1007a
$s_{K'S}(X)$
$v_{K'P}(s_{K'S}(X)) = VX$
$VX = X$
1007b
1007
1007c1
$PH_j \equiv VCK$
1007c3
INVALIDE
EK_{kj}
1007c2
$VK'_P = K'_P$
$VX = VX$
INTERRUPT PROTOCOL
1007d
CONTINUE PROTOCOL
1007e
1002

FIG. 2a.

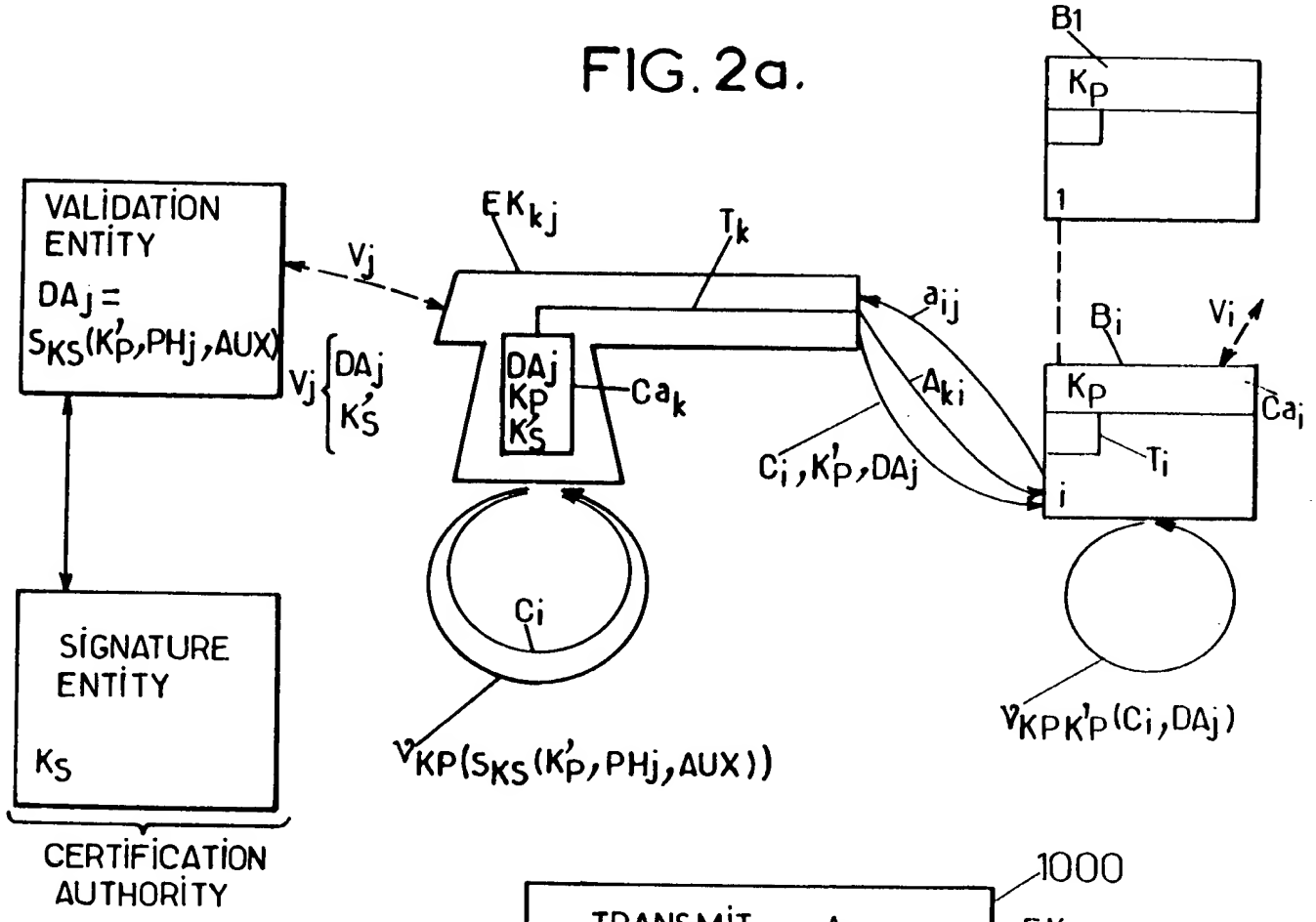

B1
K_P
1
VALIDATION ENTITY
$DA_j = S_{KS}(K'_P, PH_j, AUX)$
V_j
EK_{kj}
T_k
a_{ij}
B_i
V_i
V_j {DAj, K'_S}
DAj
K_P
K'_S
Ca_k
A_{ki}
K_P
Ca_i
C_i, K'_P, DA_j
T_i
i
C_i
SIGNATURE ENTITY
K_S
$V_{KP}(S_{KS}(K'_P, PH_j, AUX))$
$V_{KP K'P}(C_i, DA_j)$
CERTIFICATION AUTHORITY

FIG. 2b.

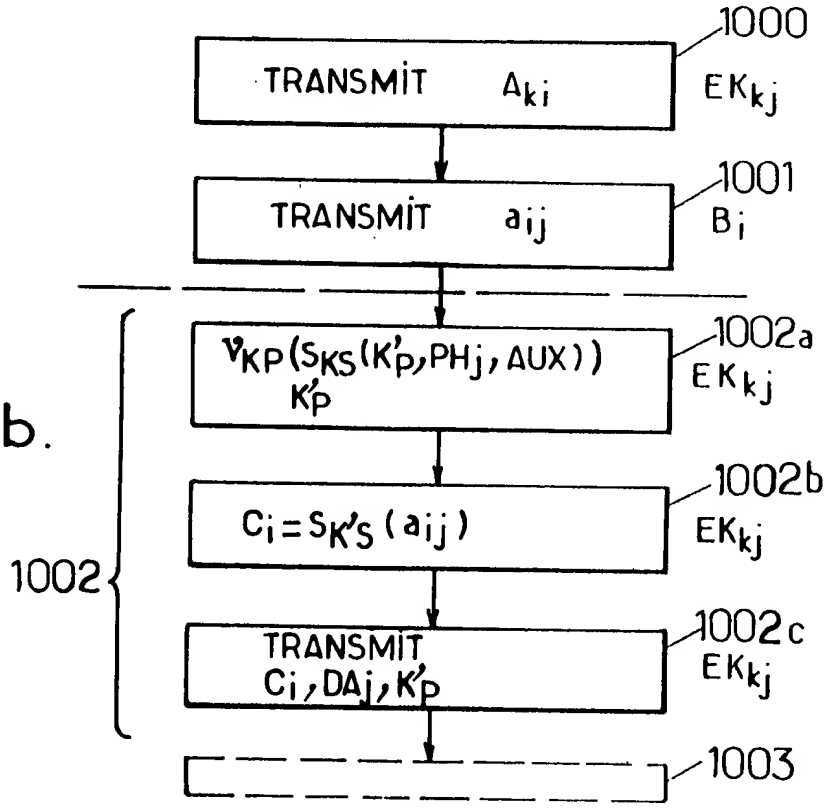
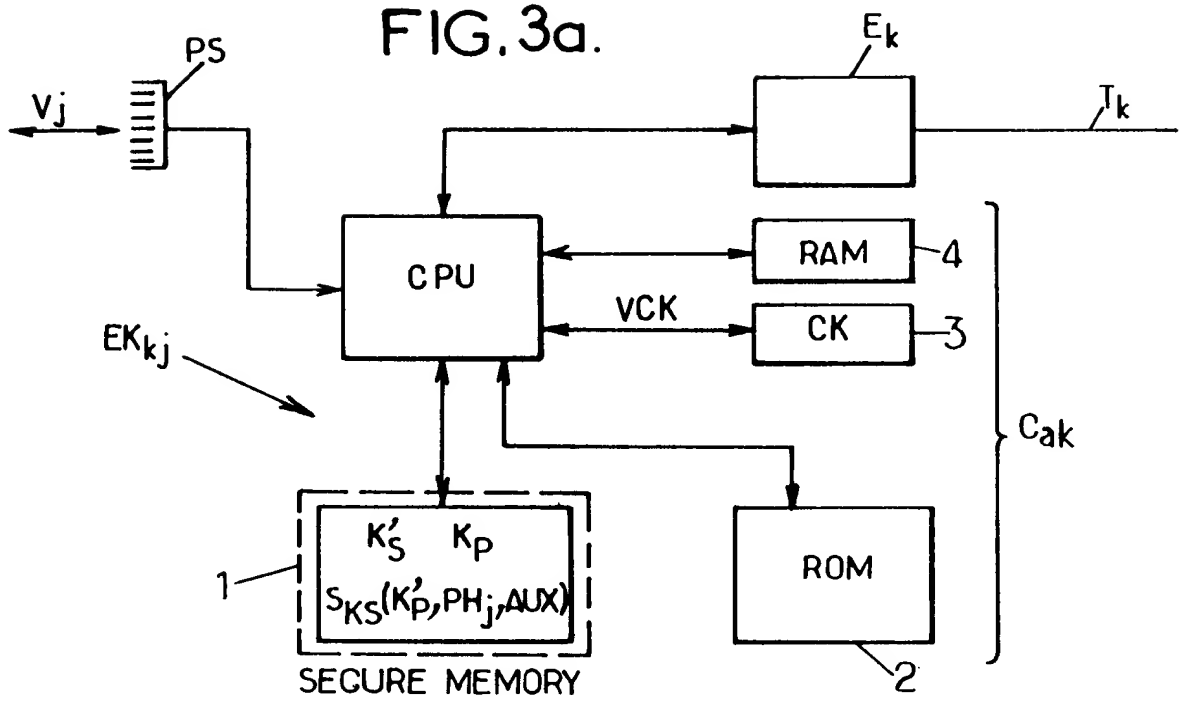

1000
TRANSMIT A_{ki}
EK_{kj}
1001
TRANSMIT a_{ij}
B_i
1002
1002a
$V_{KP}(S_{KS}(K'_P, PH_j, AUX))$
K'_P
EK_{kj}
1002b
$C_i = S_{K'S}(a_{ij})$
EK_{kj}
1002c
TRANSMIT C_i, DA_j, K'_P
EK_{kj}
1003

FIG.3a.


PS
Vj
Ek
Tk
CPU
RAM
4
VCK
CK
3
EKkj
Cak
K's KP
SKS(K'P,PHj,AUX)
1
SECURE MEMORY
ROM
2

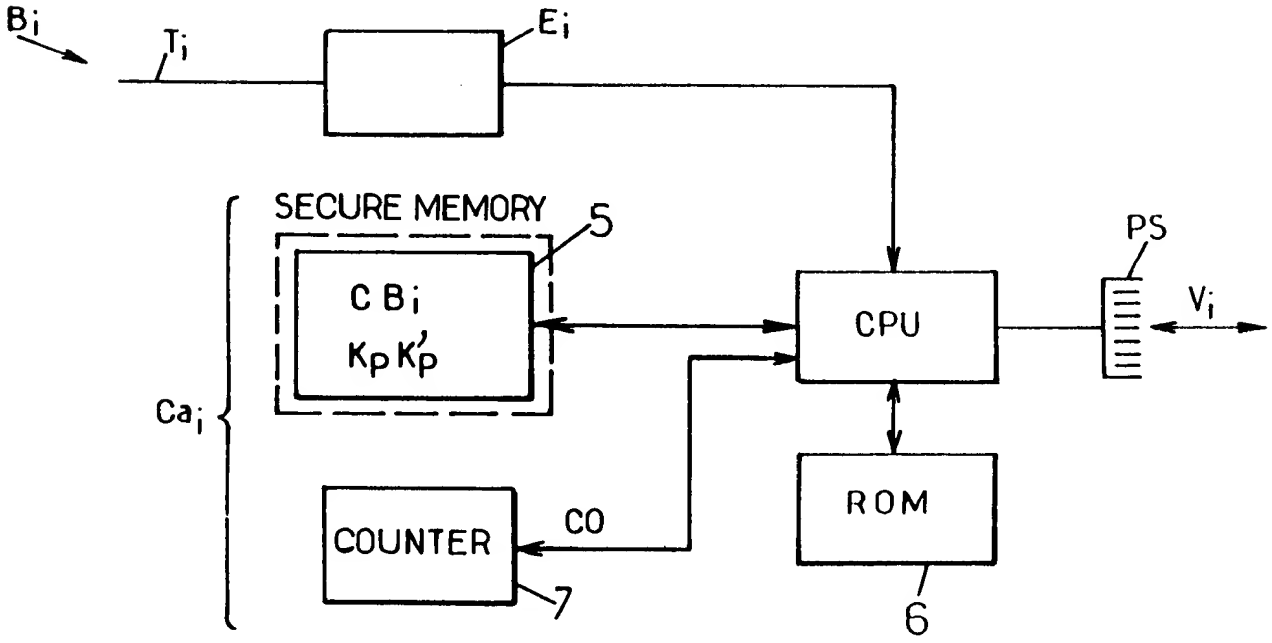

Bi
Ti
Ei
SECURE MEMORY
5
C Bi
KP K'P
PS
Vi
CPU
Cai
ROM
COUNTER
CO
7
6

FIG.3b.